PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON ENERGY AND COMMERCE
U.S. HOUSE OF REPRESENTATIVES

on

Phone Records for Sale:
Why Aren't Phone Records Safe From Pretexting?

February 1, 2006

I. Introduction

Mr. Chairman, Mr. Dingell, and members of the Committee, I am Jon Leibowitz, Commissioner of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to discuss telephone records pretexting and the Commission's significant work to protect the privacy and security of telephone records and other types of sensitive consumer information. The Commission is currently investigating companies that offer consumer telephone records for sale, and we plan to pursue these investigations vigorously.

Maintaining the privacy and security of consumers' personal information is one of the Commission's highest priorities. Companies that engage in pretexting – the practice of obtaining personal information, such as telephone records, under false pretenses – not only violate the law, but they undermine consumers' confidence in the marketplace and in the security of their sensitive data. While pretexting to acquire telephone records has recently become more prevalent, the practice of pretexting is not new. The Commission has used its full arsenal of tools to attack scammers who use fraud to gain access to consumers' personal information.

[1] The views expressed in this statement represent the views of the Commission. My oral testimony and responses to questions reflect my own views and do not necessarily represent the views of the Commission or any individual Commissioner.

Aggressive law enforcement is at the center of the FTC's efforts to protect consumers' sensitive information. The Commission has taken law enforcement action against companies allegedly offering surreptitious access to consumers' financial records, and will continue to challenge business practices that unnecessarily expose consumers' sensitive information. The Commission also continues to provide consumer education and outreach to industry to ensure that the marketplace is safe for consumers and commerce.[2]

Today I will discuss the FTC's efforts to protect consumers from firms engaged in pretexting and the practice of pretexting for telephone records.[3]

---

[2] For example, the Commission recently launched OnGuard Online, a campaign to educate consumers about the importance of safe computing. *See* www.onguardonline.gov. One module offers advice on avoiding spyware and removing it from computers. Another module focuses on how to guard against "phishing," a scam where fraudsters send spam or pop-up messages to extract personal and financial information from unsuspecting victims. Yet another module provides practical tips on how to avoid becoming a victim of identity theft. These materials are additions to our comprehensive library on consumer privacy and security. *See* www.ftc.gov/privacy/index.html.

[3] Pretexting is not the only way to obtain consumers' telephone records, however. Such records also reportedly have been obtained by bribing telephone company employees and

II. FTC Efforts to Protect Consumers From Firms That Engage in Pretexting

The Commission has a history of combating pretexting. Using Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce,"[4] the Commission has brought actions against businesses that use false pretenses to gather financial information on consumers. In these cases, we have alleged that it is a deceptive and unfair practice to obtain a consumer's financial information by posing as the consumer.

---

hacking into telephone companies' computer systems. *See, e.g.*, Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, Wash. Post, July 13, 2005, *available at* 2005 WLNR 10979279; *Simple Mobile Security for Paris Hilton*, PC Magazine, Mar. 1, 2005, *available at* 2005 WLNR 3834800.

[4] 15 U.S.C. § 45(a).

The Commission's first pretexting case was filed against a company that offered to provide consumers' financial records to anybody for a fee.[5] According to our complaint, the company's employees obtained these records from financial institutions by posing as the consumer whose records it was seeking. The complaint charged that this practice was both deceptive and unfair under Section 5 of the FTC Act.[6]

In 1999, Congress passed the Gramm-Leach-Bliley Act ("GLBA"), in large part through the efforts of this Committee. The GLBA provided another tool to attack the unauthorized acquisition of consumers' financial information.[7] Section 521 of the Act directly prohibits pretexting of customer data from financial institutions. Specifically, this provision prohibits "false, fictitious, or fraudulent statement[s] or representation[s] to an officer, employee, or agent of a financial institution" to obtain customer information of a financial institution.[8]

To ensure awareness of and compliance with the new anti-pretexting provisions of the GLBA, the Commission launched Operation Detect Pretext in 2001.[9] Operation Detect Pretext

---

[5] *FTC v. James J. Rapp and Regana L. Rapp, d/b/a Touch Tone Information, Inc.*, No. 99-WM-783 (D. Colo.) (final judgment entered June 22, 2000). *See* http://www.ftc.gov/os/2000/06/touchtoneorder.

[6] An act or practice is unfair if it: (1) causes or is likely to cause consumers substantial injury; (2) the injury is not reasonably avoidable by consumers; and (3) the injury is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

[7] *Id.* §§ 6801-09.

[8] *Id.* _ 6821.

[9] *See* FTC press release "As Part of Operation Detect Pretext, FTC Sues to Halt Pretexting" (Apr. 18, 2001), *available at* http://www.ftc.gov/opa/2001/04/pretext.htm. For more information about the cases the Commission has brought under Section 521 of the GLBA, see http://www.ftc.gov/privacy/privacyinitiatives/pretexting_enf. Since GLBA's passage, the FTC has brought over a dozen cases alleging violations of Section 521 in various contexts.

combined a broad monitoring program, the widespread dissemination of industry warning notices, consumer education, and aggressive law enforcement.

In the initial monitoring phase of Operation Detect Pretext, FTC staff conducted a "surf" of more than 1,000 websites and a review of more than 500 advertisements in print media to spot firms offering to conduct searches for consumers' financial data. The staff found approximately 200 firms that offered to obtain and sell consumers' asset or bank account information to third parties. The staff then sent notices to these firms advising them that their practices were subject to the FTC Act and the GLBA, and provided information about how to comply with the law.[10]

In conjunction with the warning letters, the Commission released a consumer alert, *Pretexting: Your Personal Information Revealed*, describing how pretexters operate and advising consumers on how to avoid having their information obtained through pretexting.[11] The alert warns consumers not to provide personal information in response to telephone calls, email, or postal mail, and advises them to review their financial statements carefully, to make certain that their statements arrive on schedule, and to add passwords to financial accounts.

---

[10] *See* FTC press release "FTC Kicks Off Operation Detect Pretext" (Jan. 31, 2001), *available at* http://www.ftc.gov/opa/2001/01/pretexting.htm.

[11] *See* http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm.

While consumer education is important, it is only part of the FTC's efforts to combat pretexting. Aggressive law enforcement is critical. The FTC therefore followed up the first phase of *Operation Detect Pretext* in 2001 with a trio of law enforcement actions against information brokers.[12] In each of these cases, the defendants advertised that they could obtain non-public, confidential financial information, including information on checking and savings account numbers and balances, stock, bond, and mutual fund accounts, and safe deposit box locations, for fees ranging from $100 to $600. The FTC alleged that the defendants or persons they hired called banks, posing as customers, to obtain balances on checking accounts.[13]

The FTC's complaints alleged that the defendants' conduct violated the anti-pretexting prohibitions of the GLBA, and further was unfair and deceptive in violation of Section 5 of the FTC Act. The defendants in each of the cases ultimately agreed to settlements that barred them from further violations of the law and required them to surrender ill-gotten gains.[14]

Because the anti-pretexting provisions of the GLBA provide for criminal penalties, the Commission also may refer pretexters to the U.S. Department of Justice for criminal prosecution,

---

[12] *FTC v. Victor L. Guzzetta, d/b/a Smart Data Systems*, No. CV-01-2335 (E.D.N.Y.) (final judgment entered Feb. 25, 2002); *FTC v. Information Search, Inc., and David Kacala*, No. AMD-01-1121 (D. Md.) (final judgment entered Mar. 15, 2002); *FTC v. Paula L. Garrett, d/b/a Discreet Data Systems*, No. H 01-1255 (S.D. Tex.) (final judgment entered Mar. 25, 2002).

[13] In sting operations set up by the FTC in cooperation with banks, investigators established dummy bank account numbers in the names of cooperating witnesses and then called defendants, posing as purchasers of their pretexting services. In the three cases, an FTC investigator posed as a consumer seeking account balance information on her fiancé's checking account. The defendants or persons they hired proceeded to call the banks, posing as the purported fiancé, to obtain the balance on his checking account. The defendants later provided the account balances to the FTC investigator.

[14] *See* http://www.ftc.gov/opa/2002/03/pretextingsettlements.htm.

as appropriate. One such individual recently pled guilty to one count of pretexting under the GLBA.[15]

[15] *United States v. Peter Easton*, No. 05 CR 0797 (S.D.N.Y.) (final judgment entered Nov. 17, 2005).

Finally, the Commission is aware that it is not enough to focus on the purveyors of illegally obtained consumer data. It is equally critical to ensure that entities that handle and maintain sensitive consumer information have in place reasonable and adequate processes to protect that data. Accordingly, the Commission has challenged data security practices as unreasonably exposing consumer data to theft and misuse.[16] Companies that have failed to implement reasonable security and safeguard processes for consumer data face liability under various statutes enforced by the FTC, including the Fair Credit Reporting Act, the Safeguards provisions of the GLBA, and Section 5 of the FTC Act.[17]

---

[16] In addition to law enforcement in the data security area, the Commission has provided business education about the requirements of existing laws and the importance of good security. *See, e.g.*, Safeguarding Customers' Personal Information: A Requirement for Financial Institutions, *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/safealrt.htm.

[17] *United States v. ChoicePoint, Inc.* (N.D. Ga.) (complaint and proposed settlement filed on Jan. 30, 2006 and pending court approval); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. 042-3160 (Sept. 20, 2005); *In the Matter of DSW, Inc.*, FTC Docket No. 052-3096 (proposed settlement posted for public comment on Dec. 1, 2005); *Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005). As the Commission has stated, an actual

breach of security is not a prerequisite for enforcement under Section 5; however, evidence of such a breach may indicate that the company's existing policies and procedures were not adequate. It is important to note, however, that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution. *See* Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft (June 16, 2005) at 6, *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

In fact, last week the Commission announced a record-breaking proposed settlement with data broker ChoicePoint, Inc. This proposed settlement requires ChoicePoint to pay $10 million in civil penalties and $5 million in consumer redress to settle charges that its security and record-handling procedures violated the Fair Credit Reporting Act and the FTC Act. In addition, the proposed settlement requires ChoicePoint to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program, and to obtain audits by an independent third-party security professional every other year until 2026. Further, the proposed settlement sends a strong signal to industry that it must maintain reasonable procedures for safeguarding sensitive consumer information and protecting it from data thieves.

III. Pretexting for Consumers' Telephone Records

An entire industry of companies offering to provide purchasers with the cellular and land line phone records of third parties recently has developed. Recent press stories report on the successful purchase of the phone records of prominent figures.[18] Although the acquisition of telephone records does not present the opportunity for immediate financial harm as the acquisition of financial records does, it nonetheless is a serious intrusion into consumers' privacy and could result in stalking, harassment, and embarrassment.[19] Although pretexting for

[18] News stories state that reporters obtained cell phone records of General Wesley Clark and cell phone and land line records of Canada's Privacy Commissioner Jennifer Stoddart. *See, e.g.*, Aamer Madhani and Liam Ford, *Brokers of Phone Records Targeted*, Chicago Trib., Jan. 21, 2006, *available at* 2006 WLNR 1167949.

[19] Albeit anecdotal, news articles illustrate some harmful uses of telephone records. For example, data broker Touch Tone Information Inc. reportedly sold home phone numbers

consumer telephone records is not prohibited by the GLBA, the Commission may bring a law enforcement action against a pretexter of telephone records for deceptive or unfair practices under Section 5 of the FTC Act.[20]

The Commission is currently investigating companies that appear to be engaging in telephone pretexting. Using the approach that proved successful in *Operation Detect Pretext*, Commission staff surfed the Internet for companies that offer to sell consumers' phone records. FTC staff then identified appropriate targets for investigation and completed undercover purchases of phone records. Commission attorneys currently are evaluating the evidence to determine if law enforcement action is warranted.

---

and addresses of Los Angeles Police Department detectives to suspected mobsters, who then used the information in an apparent attempt to intimidate the police officers and their families. *See, e.g.,* Peter Svensson, *Calling Records Sales Face New Scrutiny,* Wash. Post, Jan. 18, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/01/18/AR2006011801659.html.

[20] Under Section 13(b) of the FTC Act, the Commission has the authority to file actions in federal district court against those engaged in deceptive or unfair practices and obtain injunctive relief and other equitable relief, including monetary relief in the form of consumer redress or disgorgement of ill-gotten profits. However, the FTC Act does not authorize the imposition of civil penalties for an initial violation, unless there is a basis for such penalties, i.e., an applicable statute, rule or litigated decree.

In addition, the FTC is working closely with the Federal Communications Commission, which has jurisdiction over telecommunications carriers subject to the Communications Act.[21] Our two agencies are committed to coordinating our work on this issue, as we have done

[21] Consumer telephone records are considered "customer proprietary network information" under the Telecommunications Act of 1996 ("Telecommunications Act"), which amended the Communications Act, and accordingly are afforded privacy protections by the regulations under that Act. *See* 42 U.S.C. § 222; 47 C.F.R. §§ 64.2001- 64.2009. The Telecommunications Act requires telecommunications carriers to secure the data, but does not specifically address pretexting to obtain telephone records. Moreover, the FTC's governing statute specifically states that the Commission lacks jurisdiction over common carrier activities that are subject to the Communications Act. 15 U.S.C. § 46(a). The Commission opposed this jurisdictional gap during the two most recent reauthorization hearings. *See* http://www.ftc.gov/os/2003/06/030611reauthhr.htm; *see also* http://www.ftc.gov/os/203/06/030611learysenate.htm; http://www.ftc.gov/os/2002/07/sfareauthtest.htm.

successfully with the enforcement of the "National Do Not Call" legislation.[22]

IV. Conclusion

Protecting the privacy of consumers' data requires a multi-faceted approach: coordinated law enforcement by government agencies as well as action by the telephone carriers, outreach to educate consumers and industry, and improved security by record holders are essential for any meaningful response to this assault on consumers' privacy. Better security measures for sensitive data will prevent unauthorized access; aggressive and well-targeted law enforcement against the pretexters will deter others from further invasion of privacy; and outreach to consumers and industry will provide meaningful ways to avoid the harm to the public.

The Commission has been at the forefront of efforts to safeguard consumer information

---

[22] In addition, the Attorneys General of Florida, Illinois, and Missouri recently sued companies allegedly engaged in pretexting. *See* http://myfloridalegal.com/__852562220065EE67.nsf/0/D510D79C5EDFB4B98525710000Open&Highlight=0,telephone,records; http://www.ag.state.il.us/pressroom/2006_01/20060120.html; http://www.ago.mo.gov/newsreleases/2006/012006b.html. Several telecommunications carriers also have sued companies that reportedly sell consumers' phone records. According to press reports, Cingular Wireless, Sprint Nextel, T-Mobile, and Verizon Wireless have sued such companies. *See, e.g.*, http://www.upi.com/Hi-Tech/view.php?StoryID=20060124-011904-6403r; http://www.wired.com/news/technology/1,70027-0.html; http://news.zdnet.com/2100-1035_22-6031204.html.

and is committed to continuing our work in this area. We also are committed to working with this Committee to provide greater security and privacy for American consumers.